CA ARCserve® Replication and High Availability

Manuel des opérations pour UNIX et Linux

r16



Produits CA Technologies référencés

Ce document fait référence aux produits CA Technologies suivants :

- CA ARCserve® Replication
- CA ARCserve® High Availability (HA)

Dans ce manuel, le terme CA ARCserve RHA représente toute la famille de produits vendue auparavant sous la marque CA XOsoft Replication (WANsync) et CA XOsoft High Availability (WANsyncHA).

Informations de contact de CA

Pour une assistance technique en ligne et une liste complète des sites, horaires d'ouverture et numéros de téléphone, contactez le support technique à l'adresse http://www.ca.com/worldwide.

Table des matières

Chapitre 1 : Introduction

Ce document est destiné aux administrateurs système UNIX et Linux expérimentés, intéressés par l'implémentation et le déploiement de la solution CA ARCserve RHA dans leur environnement. Tous les détails nécessaires pour installer et désinstaller le produit, créer des scénarios de réplication (récupération après sinistre) et de haute disponibilité (HD), gérer les scénarios et récupérer des données perdues y sont fournis.

Ce chapitre traite des sujets suivants :

Documentation connexe

Utilisez ce manuel en association avec le *Manuel d'installation de CA ARCserve RHA*, le *Manuel d'administration de CA ARCserve RHA* et le *Manuel de PowerShell pour CA ARCserve RHA*.

Types de serveurs pris en charge

Pour plus d'informations sur les types de serveur pris en charge, reportez-vous aux Notes de parution.

Chapitre 2 : Installation et désinstallation de CA ARCserve RHA

Ce chapitre explique l'installation et la désinstallation du moteur et du gestionnaire CA ARCserve RHA.

Ce chapitre traite des sujets suivants :

Installation du moteur

Le progiciel d'installation CA ARCserve RHA est constitué de packages pour toutes les plates-formes prises en charge et d'un script d'installation commun.

Pour installer le moteur :

1. Devenez superutilisateur (utilisateur root).
2. Passez du répertoire de travail à celui contenant les fichiers d'installation.
3. Exécutez le script *install.sh*.
4. Suivez les instructions jusqu'à la fin de l'installation.

   Vous êtes invité à accepter le contrat de licence et à indiquer si vous souhaitez créer un groupe CA ARCserve RHA et activer la prise en charge d'Oracle.

   Remarques :

   - Si vous décidez d'activer la prise en charge d'Oracle, vous devez indiquer le propriétaire Oracle, le chemin d'installation de l'application Oracle et le chemin d'accès de base d'Oracle. Le nom d'utilisateur du propriétaire d'Oracle est requis en premier, puis l'application récupère le chemin d'installation et le chemin d'accès de base à travers l'environnement d'utilisateur du propriétaire d'Oracle. Si le chemin d'installation et le chemin d'accès de base sont introuvables, vous devez les ajouter manuellement. Si votre serveur Oracle est installé sans la bibliothèque du client Oracle 32 bits, vous devez également fournir le chemin d'accès à Oracle Instant Client.
   - Si le package CA ARCserve RHA a été installé, vous êtes invité à le réinstaller.
   - Pour permettre aux utilisateurs non-root de gérer des scénarios, vous devez créer le groupe caarha sur votre ordinateur et vérifier que le groupe est compatible avec le groupe supplémentaire.

installation du moteur dans des zones Solaris non globales

Pour les zones non globales sur Solaris, vous devez exécuter le script *configure.sh* dans chaque zone non globale

Remarque : Pour les zones non globales sous Solaris 11, vérifiez que vous avez installé le moteur RHA sur des zones globales avant de l'installer sur des zones non globales.

Pour installer le moteur dans des zones Solaris non globales :

1. Exécutez le script *install.sh* dans les zones globales comme processus supérieur.
2. Exécutez le script *configurez. sh* dans chaque zone non globale après l'installation.

Gestion du moteur

Après l'installation, le moteur CA ARCserve RHA est géré automatiquement par le système d'exploitation : il est démarré pendant la séquence de démarrage du système et arrêté pendant le processus de fermeture de celui-ci. Ces procédures sont exécutées automatiquement au moyen de scripts **.rc**.

Toutefois, si vous devez arrêter manuellement le moteur, puis le redémarrer, procédez comme suit.

Linux

Pour lancer un moteur :

```
/etc/init.d/ARCserveRHA start
```

Pour arrêter un moteur :

```
/etc/init.d/ARCserveRHA stop
```

Solaris

Pour lancer un moteur :

```
/etc/init.d/ARCserveRHA start
```

Pour arrêter un moteur :

```
/etc/init.d/ARCserveRHA stop
```

AIX

Pour lancer un moteur :

```
/opt/CA/ARCserveRHA/bin/ARCserveRHA.rc start
```

Pour arrêter un moteur :

```
/opt/CA/ARCserveRHA/bin/ARCserveRHA.rc stop
```

Installation du gestionnaire

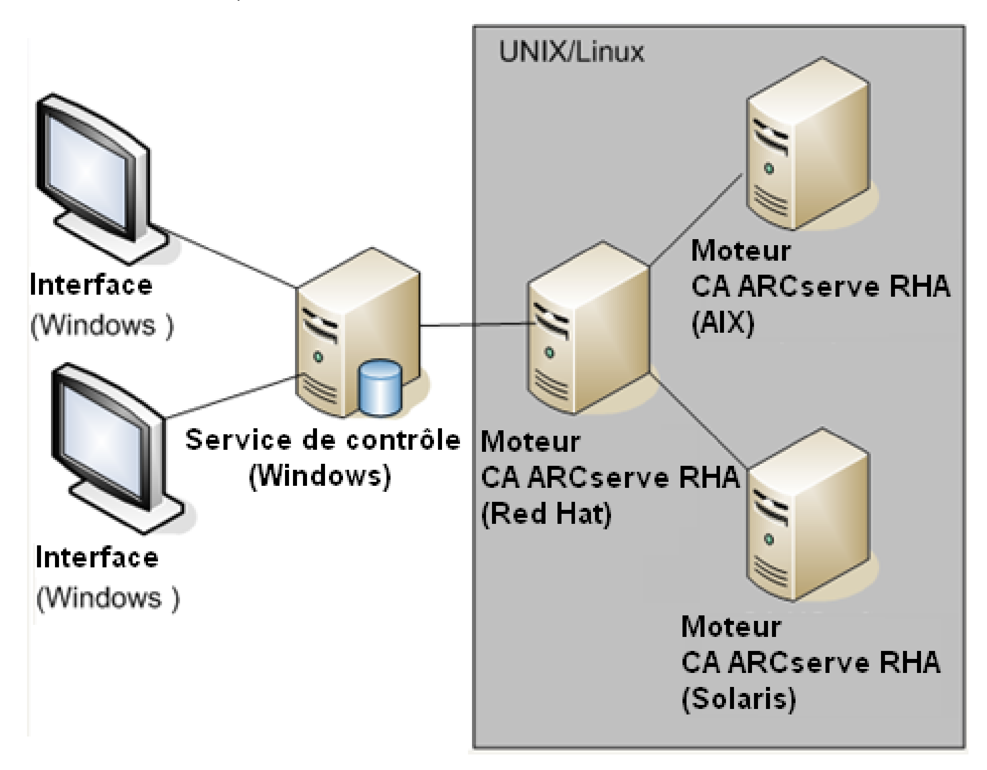
Le gestionnaire CA ARCserve RHA est installé uniquement sur les plates-formes Windows. L'installation des composants CA ARCserve RHA sous Windows est très simple. Le package d'installation contient un fichier appelé *Setup.exe* qui exécute un assistant MSI standard.

- Cette installation (logicielle) ne nécessite ni arrêt des applications, ni redémarrage du système.
- Le niveau requis pour *instmsi.exe* est 2.0.2600.2 (ou versions ultérieures). Si cette condition n'est pas remplie, le programme d'installation de CA ARCserve RHA procède automatiquement à la mise à niveau du programme d'installation de Windows. Toutefois, cette mise à niveau exige un redémarrage.

Des invites standard vous guident lors de l'installation. Votre seule décision importante consiste à choisir les serveurs sur lesquels installer les applications. Le gestionnaire CA ARCserve RHA et CA ARCserve RHA PowerShell sont installés ensemble :

- Installez le gestionnaire et le service de contrôle CA ARCserve RHA sur n'importe quel ordinateur Windows Server doté d'un accès aux ordinateurs que vous souhaitez gérer, comme l'illustre le diagramme ci-dessous.
- Le répertoire d'installation par défaut (INSTALLDIR) est \Program Files\CA\ARCserve RHA. Tous les fichiers exécutables, DLL et fichiers de configuration se trouvent dans le répertoire INSTALLDIR.
- Un utilisateur Windows exécutant le gestionnaire CA ARCserve RHA a besoin des droits en lecture et en écriture sur le répertoire d'installation.

Installez le moteur CA ARCserve RHA sur tous les serveurs participant à des scénarios UNIX/Linux. Pour plus d'informations sur l'installation du gestionnaire CA ARCserve RHA, consultez le *Manuel d'installation de CA ARCserve RHA*.



Préparation de l'environnement pour la haute disponibilité avec le script GSSnsupdate

Pour exécuter des scénarios de haute disponibilité dans des domaines de zone DNS, configurez votre serveur UNIX ou Linux pour qu'il puisse authentifier et modifier les enregistrements de l'hôte DNS A pour les serveurs maître et de réplication dans des scénarios.

Vous pouvez configurer votre environnement UNIX/Linux pour CA ARCserve RHA à l'aide du script Perl inclus. Pour obtenir d'autres versions de ce script, contactez le support.

Les étapes suivantes doivent être effectuées sur tous les hôtes UNIX/Linux de votre environnement.

Pour préparer les hôtes UNIX et Linux pour la haute disponibilité dans les domaines de zone DNS sécurisée :

1. Configurez l'hôte Linux en tant que client Kerberos. Pour cela, modifiez le fichier /etc/krb5.conf comme suit :

```
[libdefaults]
default_realm = <nom_domaine, par ex. XOSOFT.ORG>

[realms]
 <nom_domaine> = {
  kdc = <nom_domaine_complet_serveur_contrôleur_domaine>:88
  admin_server = <nom_domaine_complet_serveur_contrôleur_domaine>
  default_domain = <nom_domaine, par ex. XOSOFT.ORG>
 }

[domain_realm]
. <nom_domaine>=<NOM_DOMAINE>              par ex. .xosoft.org=XOSOFT.ORG
```

```
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = XOLAB.COM

[realms]
 XOLAB.COM = {
  kdc = server01 .xolab.com:88
  admin_server = server01 .xolab.com:749
  default_domain = XOLAB.COM
 }

[domain_realm]
 .xolab.com = XOLAB.COM

[kdc]
 profile = /var/kerberos/krb5kdc/kdc.conf
```

2. Créez un fichier keytab avec ktpass sur le contrôleur de domaine spécifié dans le paramètre kdc de l'étape précédente. Connectez-vous sous un compte d'administrateur de domaines sur le KDC.

   Remarque : Par défaut, l'utilitaire ktpass n'est pas chargé sur Windows. Vous pouvez l'obtenir à partir du package Outils de support de Windows.

   ```
   ktpass -princ host/<nom_choisi@DOMAINE> -mapuser <admin_domaine@DOMAINE> -pass <mot_passe> -out c:\ <nom_fichier>.keytab -ptype KRB5_NT_PRINCIPAL
   ```

   ```
   C:\>ktpass -princ host/xodemo@XOLAB.COM -mapuser testuser@XOLAB.COM -pass qazwsx
    -out C:\xodemo.keytab -ptype KRB5_NT_PRINCIPAL
   Targeting domain controller: calabdc01.xolab.com
   Successfully mapped host/xodemo to testuser.
   Key created.
   Output keytab to C:\xodemo.keytab:
   Keytab version: 0x502
   keysize 48 host/xodemo@XOLAB.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 4 etype 0x3 (DE
   S-CBC-MD5) keylength 8 (0x8545b3195d835497)
   Account testuser has been set for DES-only encryption.

   C:\>
   ```

3. Transfert sécurisé du fichier <nom_fichier>.keytab sur l'hôte Linux

4. Sur l'hôte Linux, combinez le fichier keytab dans un fichier unique appelé /etc/krb5.keytab, au moyen du programme ktutil. Vous devrez peut-être installer le package Ktutil en premier.

   ```
   [root@server01-1x1 bin]# ktutil

   ktutil:  rkt /root/ <filename>.keytab

   ktutil:  wkt /etc/krb5.keytab

   ktutil:  list

   ktutil: q
   ```

   ```
   [root@ server01  -1x1 ~]# /usr/kerberos/sbin/ktutil
   ktutil:  rkt ./xodemo.keytab
   ktutil:  wkt /etc/krb5.keytab
   ktutil:  list
   slot KVNO Principal
   ---- ---- ---------------------------------------------------------------------
      1    5                      host/test@XOLAB.COM
   ktutil:  q
   [root@calabsrv07-1x1 ~]#
   ```

5. Assurez-vous que l'heure de l'hôte Linux est synchronisé avec le serveur NTP ou avec le serveur Microsoft DNS.

6. Copiez le script Perl nsupdate-gss.pl et installez l'ensemble des bibliothèques Perl requises par le script. Ces sources Perl sont disponibles à l'adresse http://search.cpan.org ou via un RPM.

   ```
   perl-Digest-HMAC
   perl-Net-IP
   perl-Net-DNS
   perl-GSSAPI
   perl-Krb5…
   ```

7. Modifiez le nom principale du keytab Kerberos dans le script nsupdate-gss.pl situé à /opt/CA/ARCserve RHA/ pour faire correspondre le nom que vous avez choisi ci-dessus, par exemple hôte/xodemo.

```
#############################
my $sys_retcode = system("kinit -k hôte/xodemo");
if ($sys_retcode != 0) {
        print "Failt to create and cache Kerberos ticket through 'kinit'\n";
        exit 1;
}

#############################
```

8. Exécutez le test suivant pour vous assurer que l'environnement est prêt et que le script peut mettre à jour les enregistrements A DNS.

```
./nsupdate-gss.pl 192.168.88.1 shagu01-RHEL5u3-x64 xosoft.org --
add_ips=192.168.88.21 --ttl=60 --del_ips=192.168.88.31
```

9. Pour effectuer une mise à jour sécurisée sur Microsoft DNS, définissez le script nsupdate-gss.pl dans le fichier ws_rep.cfg situé dans le répertoire d'installation /opt/CA/ARCserveRHA/bin. Supprimez le # en face de la ligne GSSNsupdateScript = :

```
####################
# Script permettant une mise à jour sécurisée dynamique sur le serveur MS DNS
sur des hôtes UNIX/Linux
GSSNsupdateScript = "[INSTALLDIR]/scripts/nsupdate-gss.pl"
#
# Vous pouvez consulter le support CA à l'adresse http://support.ca.com/ pour
obtenir de l'aide ou
# pour définir le script par commande shell ou en Perl avec les arguments
correspondant à
# GSSNsupdateScript NAME_SERVER HOST DOMAIN [options]
# Options :
#         -- add_ips=IPS       IPs cibles pour les enregistrements A à
ajouter
#         -- ttl=TTL           durée de vie pour les enregistrements A à
ajouter
#         -- del_ips=IPS       IPs cibles pour les enregistrements A à
supprimer
```

10. Arrêtez et redémarrez le moteur :

```
/etc/init.d/ARCserveRHA stop

/etc/init.d/ARCserveRHA start
```

11. Répétez cette procédure pour l'autre hôte.

Mise à niveau de CA ARCserve RHA

Avant de procéder à la mise à niveau vers cette version, prenez en compte les éléments suivants :

- Arrêtez tous les scénarios en cours d'exécution.
- Vous n'avez pas besoin de désinstaller manuellement la version antérieure. Le processus d'installation supprime automatiquement la version précédente.
- Copiez les anciens scénarios sur l'ordinateur qui exécute cette version de l'interface utilisateur graphique de gestion CA ARCserve RHA Une fois copiés, ces scénarios peuvent être importés dans cette version de CA ARCserve RHA en sélectionnant le menu Scénario, Importer. Les scénarios peuvent se trouver à l'emplacement ci-dessous.
  - UNIX : /opt/CA/ARCserveRHA/bin/ws_scenarios
  - Windows : Program Files (x86)/CA/ARCserve RHA/Manager/ws_scenarios

Désinstallation de CA ARCserve RHA

Avant de désinstaller CA ARCserve RHA, vous devez arrêter tous les scénarios en cours d'exécution et vérifier qu'aucun répertoire n'est monté par xofs.

Pour vérifier qu'aucun répertoire n'est monté par xofs, assurez-vous que le fichier /etc/xofs_mnttab est vide. Si ce n'est pas le cas, reportez-vous à la section *Déchargement des pilotes xofs* (page 37).

Remarque : Vous pouvez ignorer le processus de vérification si vous redémarrez votre ordinateur à la fin de la procédure de désinstallation.

Désinstaller CA ARCserve RHA

Pour désinstaller CA ARCserve RHA sur toutes les plates-formes UNIX/Linux prises en charge, utilisez la procédure suivante.

Pour désinstaller CA ARCserve RHA :

1. Devenez superutilisateur.
2. Vérifiez que tous les scénarios de réplication sont arrêtés.
3. Exécutez le script de désinstallation suivant :

   ```
   /opt/CA/ARCserveRHA/bin/uninstall.sh
   ```

   Vous êtes invité à confirmer la procédure de désinstallation. Par exemple : *uninstall CA ARCserve RHA (y/n)*
4. Saisissez *y* et appuyez sur la touche Entrée.
5. [Facultatif] Redémarrez.

Chapitre 3 : Méthodes de redirection

CA ARCserve High Availability (CA ARCserve HA) permet de surveiller tous les événements stratégiques, y compris les défaillances globales des serveurs ainsi que toutes les défaillances des services de base de données, et de lancer une permutation automatique ou manuelle.

Lorsque le serveur maître devient indisponible, ses activités peuvent être permutées automatiquement vers un site distant (ordinateur de réplication). Transparente pour l'utilisateur, la permutation provoque le démarrage immédiat d'une base de données synchronisée en attente et la redirection, en un temps minimum, de tous les utilisateurs vers cette base de données. Cette opération s'exécute sans reconfiguration des clients ou du réseau.

La redirection peut être basée sur les méthodes suivantes :

- Transfert IP, si le site de secours est implémenté dans le même segment réseau.
- Redirection du système DNS, qui peut être utilisée sur un réseau local ou lorsque le site de secours distant est situé sur un autre réseau IP (permutation multiréseau).
- Basculement du nom d'hôte de serveur

Remarque : Vous pouvez également appliquer des scripts définis par l'utilisateur pour ajouter ou remplacer les méthodes de redirection intégrées. Des scripts d'identification de la direction du trafic réseau sont nécessaires pour prendre totalement en charge les méthodes de redirection personnalisées. Les scripts ou les fichiers de commandes personnalisés sont utilisés pour identifier le serveur actif. Ce script détermine si le lancement du scénario exécute un scénario avant ou arrière. Le script s'exécute sur les ordinateurs maître et de réplication : celui qui renvoie zéro est actif. Si les deux renvoient zéro, un conflit est signalé.

La sélection de la méthode de redirection est basée sur la configuration requise par l'application faisant l'objet de la protection ; certaines méthodes peuvent ne pas s'appliquer à un scénario spécifique. Pour plus d'informations, consultez le Manuel des opérations correspondant à l'application.

Si vous utilisez la méthode de basculement de nom d'hôte pour la redirection dans des scénarios UNIX/Linux, vous devez également définir la redirection de système DNS.

Remarque : Pour la méthode de redirection Transfert IP sur des plates-formes Linux, configurez l'adresse IP uniquement à l'aide de la commande ifconfig.

Chapitre 4 : Scénarios de gestion

Cette section décrit la création, le démarrage et l'arrêt de scénarios à l'aide du gestionnaire. Vous pouvez également utiliser PowerShell pour gérer vos scénarios. Pour plus d'informations sur l'utilisation de PowerShell pour créer un scénario, reportez-vous au *Manuel de PowerShell pour CA ARCserve RHA*.

Important : CA ARCserve RHA est particulièrement adapté à la réplication de fichiers de données. Il n'est cependant pas recommandé pour répliquer des fichiers exécutables et des bibliothèques, car cela risque d'affecter les performances des applications. Pendant la création d'un scénario, vous pouvez exclure ces fichiers de la réplication.

Dans cette version, vous pouvez utiliser des scénarios de haute disponibilité pour protéger votre environnement UNIX.

Ce chapitre traite des sujets suivants :

Création d'un scénario de réplication UNIX

La protection d'ordinateurs UNIX et Linux à l'aide de CA ARCserve RHA nécessite des scénarios de réplication qui identifient les serveurs maître et de réplication, ainsi que les propriétés contrôlant le comportement des scénarios. Vous pouvez créer des scénarios de serveur de fichiers ou Oracle, selon les besoins. La détection automatique permet de protéger une seule instance Oracle dans un seul scénario. Si plusieurs instances Oracle doivent être protégées dans un même scénario, utilisez le type de scénario de serveur de fichiers. La création de scénarios est un processus reposant sur un assistant ; les étapes de création de scénarios de serveur de fichiers et Oracle se ressemblent beaucoup. Les différences qui existent sont clairement indiquées. Pour obtenir des instructions plus détaillées, reportez-vous au manuel des opérations approprié.

Remarque : Les répertoires racines ne peuvent pas être croisés dans des scénarios différents. Vous ne pouvez pas créer un deuxième scénario de réplication utilisant le répertoire maître et le répertoire racine utilisés pour votre premier scénario.

Utilisez votre navigateur Web pour vous connecter à CA ARCserve RHA à l'aide du service de contrôle, connectez-vous à la page du portail et exécutez l'interface utilisateur graphique de gestion. Si vous exécutez l'interface utilisateur graphique pour la première fois, celle-ci s'installe automatiquement grâce à la technologie ClickOnce™. Vous trouverez ci-dessous l'URL de la page du portail.

http://<HôteServiceContrôle>:8088/entry_point.aspx

1. Dans le gestionnaire, sélectionnez Scénario, puis Nouveau ou cliquez sur Nouveau scénario dans la barre d'outils.

   L'assistant de création de scénarios s'affiche.

2. Sélectionnez Créer un scénario, puis cliquez sur Suivant.

   La boîte de dialogue Sélection d'un serveur et d'un type de produit s'ouvre.

3. Sélectionnez les options de scénarios appropriées comme suit :

   a. Dans la liste Sélection du type de serveur, sélectionnez le type de scénario que vous souhaitez créer. Pour la réplication UNIX/Linux, seuls les scénarios de serveur de fichiers et Oracle sont pris en charge.

   b. Dans les options Sélection du type de produit, sélectionnez Scénario de réplication et de récupération des données.

4. Cliquez sur Suivant.

   La boîte de dialogue Hôtes maître et de réplication s'ouvre.

5. Saisissez les noms ou les adresses IP des serveurs maître et de réplication à protéger, puis cliquez sur Suivant.

   La boîte de dialogue Vérification du moteur s'affiche. Patientez pendant la vérification du statut de la version du moteur. Si la version actuelle est dépassée, CA ARCserve RHA vous demande si vous souhaitez effectuer la mise à jour. Vous pouvez installer la dernière version ou continuer. Une fois la vérification terminée, cliquez sur Suivant.

   Remarque : S'il s'agit d'un scénario de type Oracle, vous êtes invité à indiquer vos informations d'identification. Vous devez saisir les informations d'identification d'un compte doté des droits d'administration sur la base de données afin que CA ARCserve RHA puisse interroger la configuration Oracle sur le serveur maître.

6. Saisissez le nom de l'instance Oracle, le DBA Oracle et le nom d'utilisateur/mot de passe, puis cliquez sur OK.

   - Dans les scénarios de **serveur de fichiers**, la boîte de dialogue Répertoires racines de l'ordinateur maître s'affiche. Sélectionnez les fichiers et/ou les répertoires à répliquer à partir de l'ordinateur maître, puis cliquez sur Suivant pour accéder à la fenêtre Répertoires racines de l'ordinateur de réplication.

   - Dans les scénarios **Oracle**, la boîte de dialogue Sélection d'espaces disque logiques pour la réplication s'affiche à la place de la boîte de dialogue Répertoires racines de l'ordinateur maître. CA ARCserve RHA fournit une liste de résultats détectés automatiquement sur le serveur maître. Sélectionnez ou désélectionnez selon vos besoins, les bases de données pour la réplication, puis activez l'option Répliquer les fichiers créés par l'utilisateur dans les répertoires racines de la liste. Cliquez sur Suivant pour accéder à la fenêtre Répertoires racines de l'ordinateur de réplication.

   La boîte de dialogue Répertoires racines de l'ordinateur de réplication s'ouvre. En fonction du type de scénario que vous créez, la boîte de dialogue Répertoires racines de l'ordinateur de réplication affiche une liste de répertoires pour la base de données Oracle ou le serveur de fichiers.

7. Sélectionnez les fichiers et/ou les répertoires à partir de l'ordinateur de réplication sur lequel les données à répliquer seront stockées, puis cliquez sur Suivant.

   Remarque : Si la structure des répertoires est identique sur le serveur de réplication, l'assistant la sélectionne automatiquement comme répertoire où répliquer les données.

La boîte de dialogue Propriétés du scénario s'ouvre.

8. Configurez la page Propriétés des hôtes maître et de réplication. En général, les valeurs par défaut sont appropriées. Vous pouvez modifier tous les paramètres de ce volet une fois le scénario créé.

   Remarque : Le spool est un dossier du disque utilisé pour le stockage temporaire des données à répliquer. Les paramètres du spool, situés dans l'onglet Propriétés (à la fois sur l'hôte maître et sur celui de réplication) ou définis à l'aide de l'assistant de création de scénarios, déterminent la quantité d'espace disque disponible pour le spool. Dans la plupart des cas, les valeurs par défaut sont suffisantes. Toutefois, si vous choisissez de modifier cette valeur, elle doit représenter au moins 10 % de la taille totale de l'ensemble de données. Pour plus d'informations, consultez le *Manuel d'administration de CA ARCserve RHA*.

   La boîte de dialogue Propriétés des ordinateurs maître et de réplication s'ouvre.

9. Pour permettre la récupération de données perdues à partir de l'hôte de réplication à l'aide de points de retour arrière, définissez l'option Retour arrière des données sur *Activé(e)* dans le volet Propriétés de l'hôte de réplication. Pour plus d'informations sur l'utilisation du retour arrière des données, reportez-vous à la section Retour arrière des données.

10. Une fois que les propriétés des hôtes maître et de réplication vous conviennent, cliquez sur Suivant.

    La boîte de dialogue Vérification du scénario s'affiche et l'assistant vérifie la configuration du scénario.

11. Si le scénario est correct, cliquez sur Suivant. Si des erreurs s'affichent, cliquez sur le bouton Précédent et corriger les paramètres.

    Une fois qu'il est vérifié, la page Exécution du scénario vous invite à exécuter le scénario. L'exécution du scénario démarre le processus de synchronisation des données.

12. Pour exécuter le scénario, cliquez sur Exécuter. Pour exécuter le scénario ultérieurement, cliquez sur Terminer.

    Le processus de synchronisation démarre.

Pour les zones non globales sous Solaris

Créez plusieurs scénarios dans la zone globale et gérez tous les scénarios à partir de cet endroit. La plupart des étapes sont identiques sauf les étapes suivantes :

1. Entrez l'adresse IP de la zone globale en tant qu'adresse IP principale.
2. Pour obtenir les informations de la zone et du répertoire racine de la zone, saisissez les commandes suivantes :

   ```
   /usr/sbin/zoneadm list –vi
   ```

   ```
   zonecfg -z <nom_zone> info
   ```

3. Lorsque vous définissez le répertoire racine, ajoutez manuellement le répertoire racine de la zone non globale au chemin d'accès que vous voulez protéger. Vous ne pouvez alors pas utiliser la détection automatique pour les applications telles qu'Oracle.

Création d'un scénario de haute disponibilité UNIX

Pour créer des scénarios de haute disponibilité UNIX, utilisez l'assistant de création de scénarios comme pour tous les scénarios HD.

Pour plus d'informations sur la création de scénario de haute disponibilité pour une base de données Oracle, consultez le *Manuel des opérations CA ARCserve RHA pour Oracle Server*.

Pour créer un scénario de haute disponibilité UNIX

1. Démarrez le gestionnaire CA ARCserve RHA. Sélectionnez Fichier, Créer, Nouveau scénario ou cliquez sur le bouton Nouveau scénario.

   La boîte de dialogue Bienvenue s'ouvre.

2. Cliquez sur Créer un scénario et saisissez un nom de groupe de scénarios, ou sélectionnez-en un dans la liste, puis cliquez sur Suivant.

   La boîte de dialogue Sélection d'un serveur et d'un type de produit s'ouvre.

3. Sélectionnez l'option Serveur de fichiers et vérifiez que le type de produit sélectionné est Scénario de haute disponibilité. Pour Tâches sur l'ordinateur de réplication, sélectionnez Aucun(e) et cliquez sur Suivant.

   La boîte de dialogue Hôtes maître et de réplication s'ouvre.

4. Saisissez un nom de scénario, entrez le nom d'hôte ou l'adresse IP, ainsi que le numéro de port des serveurs maître et de réplication, activez l'option Vérifier le moteur CA ARCserve RHA sur les hôtes, puis cliquez sur Suivant. Vous serez peut-être invité à indiquer les informations d'identification de l'utilisateur. Si c'est le cas, saisissez les informations d'identification adéquates et cliquez OK.

   Si vous avez activé l'option de vérification du moteur, la boîte de dialogue Vérification du moteur s'affiche.

5. Patientez pendant que la vérification se termine, puis cliquez sur Suivant pour poursuivre l'opération.

   La boîte de dialogue Répertoires racines de l'ordinateur maître s'ouvre, en affichant la liste de répertoires identifiés sur le l'ordinateur maître.

6. Cliquez sur Suivant.

   La fenêtre Répertoires racines de l'ordinateur de réplication s'affiche.

7. Définissez les propriétés du répertoire de l'ordinateur de réplication, puis cliquez sur Suivant.

   La fenêtre Propriétés du scénario s'ouvre.

8. Configurez les propriétés, puis cliquez sur Suivant. Pour plus d'informations sur la configuration des propriétés de scénario, consultez le *Manuel d'administration de CA ARCserve RHA*.

   La fenêtre Propriétés des ordinateurs maître et de réplication s'ouvre.

9. Configurez les propriétés, puis cliquez sur Suivant. Pour plus d'informations sur la configuration des propriétés des hôtes maître et de réplication, consultez le *Manuel d'administration de CA ARCserve RHA*.

   La fenêtre Propriétés de permutation s'ouvre.

10. Configurez les propriétés de permutation, puis cliquez sur Suivant.

    Remarque : Les valeurs par défaut recommandées sont déjà définies. Pour plus d'informations sur la configuration des propriétés de permutation, consultez le *Manuel d'administration de CA ARCserve RHA*.

    1. La fenêtre Démarrage de la permutation et de la réplication inversée s'affiche.

11. Pour contrôler automatiquement la permutation et la réplication inversée, sélectionnez les valeurs des options suivantes, puis cliquez sur Suivant.

    Lancement de la permutation

    Permet de spécifier si le lancement de la permutation est automatique ou manuel. La permutation automatique est lancée lorsque le serveur maître est hors service ou lorsqu'une défaillance de base de données est détectée. La permutation manuelle est lancée par l'administrateur. Dans les deux cas, un message de notification est renvoyé lorsqu'une défaillance est détectée.

    Démarrage de la réplication inversée

    Permet de spécifier si le lancement de la réplication inversée est automatique ou manuel. Après une permutation, le scénario s'arrête et la réplication inversée est lancée.

    Remarque : Il est recommandé de ne **pas** définir ces deux options sur Automatique dans un environnement de production.

    La boîte de dialogue Vérification du scénario s'affiche.

12. Patientez jusqu'à la fin du processus de vérification du scénario.

Si la vérification de scénario répertorie des erreurs, vous devez les résoudre avant de continuer. Si des avertissements sont répertoriés, vous devez également les résoudre pour pouvoir continuer. Après avoir apporté les modifications nécessaires, cliquez sur Réessayer pour répéter la vérification.

13. Cliquez sur Suivant.

    La boîte de dialogue Exécution du scénario s'ouvre.

14. Cliquez sur Exécuter pour démarrer la synchronisation et activer le scénario. Cliquez sur Terminer pour exécuter le scénario ultérieurement.

Pour les zones non globales sous Solaris

Créez plusieurs scénarios dans la zone globale et gérez tous les scénarios à partir de cet endroit. La plupart des étapes sont identiques sauf les étapes suivantes :

1. Entrez l'adresse IP de la zone globale en tant qu'adresse IP principale.
2. Pour obtenir les informations de la zone et du répertoire racine de la zone, saisissez les commandes suivantes :

   ```
   /usr/sbin/zoneadm list –vi
   ```

   ```
   zonecfg -z <nom_zone> info
   ```

3. Lorsque vous définissez le répertoire racine, ajoutez manuellement le répertoire racine de la zone non globale au chemin d'accès que vous voulez protéger. Vous ne pouvez alors pas utiliser la détection automatique pour les applications telles qu'Oracle.

Démarrage d'un scénario

Vous pouvez démarrer un scénario à l'aide du gestionnaire.

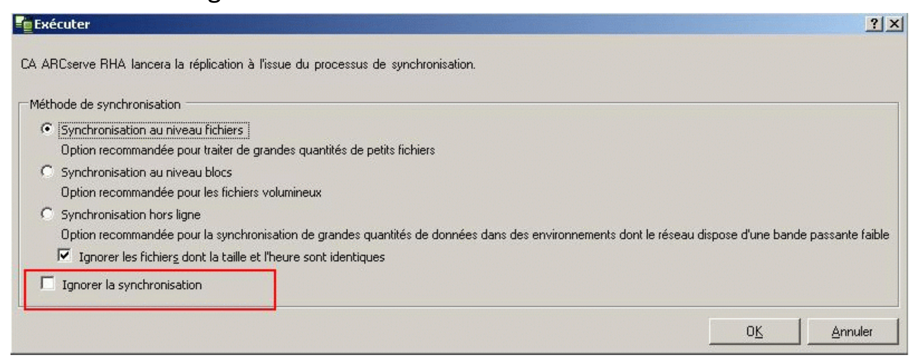
Pour démarrer un scénario :

1. Dans le volet Scénario, sélectionnez le scénario à exécuter.
2. Cliquez sur Exécuter dans la barre d'outils.

   La boîte de dialogue Résultats de la vérification s'affiche et vous invite à approuver l'exécution du scénario.

3. Cliquez sur Exécuter. Pour afficher les détails du scénario des ordinateurs maître et de réplication, cliquez sur Avancé.

   La boîte de dialogue Exécuter s'ouvre.

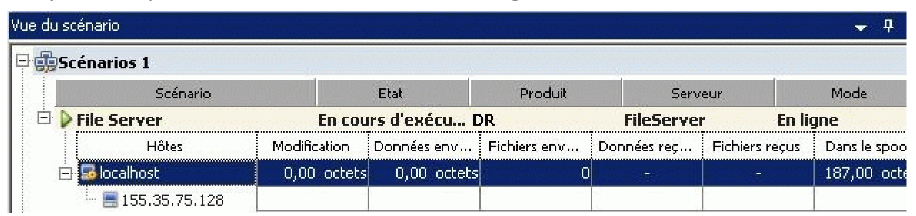


   Remarque : Lorsque vous démarrez des scénarios UNIX, vous ne pouvez pas ignorer la synchronisation au niveau fichiers ou blocs.

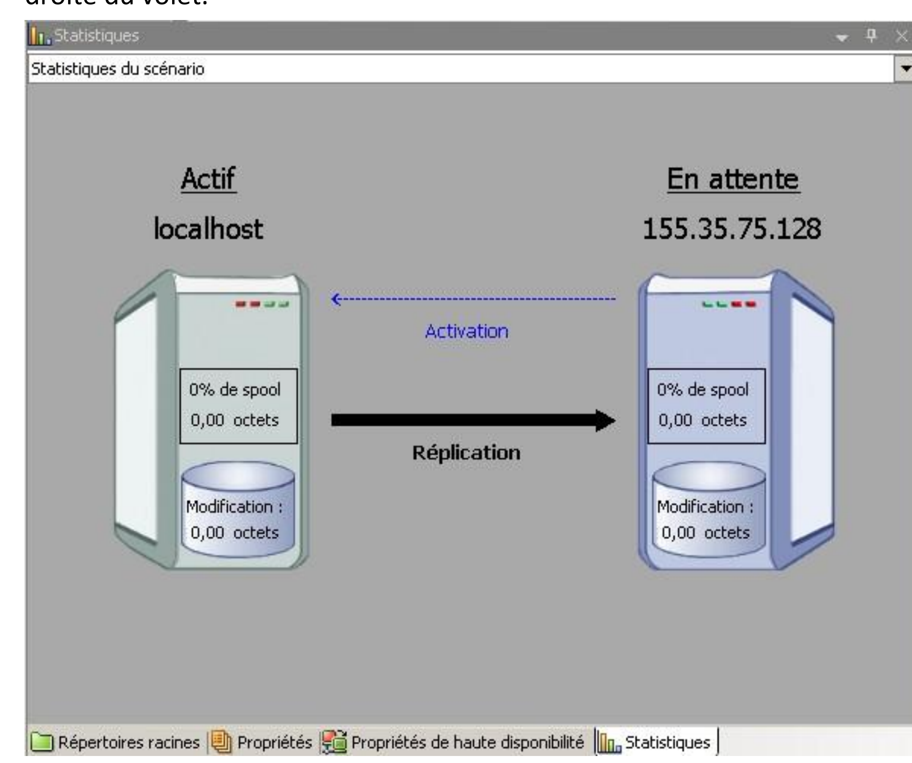
4. Choisissez Synchronisation au niveau fichiers et cliquez sur OK.

   Remarque : Si vous exécutez un scénario pour un serveur Oracle, désélectionnez la case à cocher Ignorer les fichiers dont la taille et l'heure sont identiques et sélectionnez Synchronisation au niveau blocs.

   Le gestionnaire indique alors que le scénario est en cours d'exécution, au moyen du symbole de lecture vert situé à gauche du scénario.



Une fois que le scénario s'exécute, un onglet Statistiques apparaît, en bas à droite du volet.



Lors de la synchronisation, un rapport est également généré par défaut.

Arrêt d'un scénario

Vous pouvez arrêter un scénario à l'aide du gestionnaire.

Pour arrêter un scénario :

1. Cliquez sur le bouton Arrêter dans la barre d'outils.

   Un message de confirmation apparaît, vous invitant à approuver l'arrêt du scénario.

2. Cliquez sur Yes (Oui).

   Le scénario s'arrête.

   Remarque : Une fois le scénario arrêté, le gestionnaire n'affiche plus le symbole de lecture vert à gauche du scénario et l'onglet Statistiques n'est plus disponible.

Remarques sur les scénarios UNIX/Linux

Tenez compte des éléments ci-dessous lors de la création de scénarios UNIX/Linux.

- Un répertoire ne peut être présent que dans un seul scénario.
- Pour NFS (Network File Sharing), V4 n'est pas pris en charge. Vous devez installer le moteur sur le serveur NFS et vous assurer que le répertoire exporté se trouve dans le répertoire racine.
- Le système NFS n'est pas pris en charge par SUSE 11.
- Pour la réplication de Windows vers UNIX, les listes de contrôle d'accès Windows sont perdues.
- Pour la réplication UNIX vers Windows, les UID, les GUID, les liens symboliques et les liens physiques sont perdus.
- Les noms de fichiers sous Windows ne sont pas sensibles à la casse ; des conflits peuvent donc survenir.
- Les répertoires racines ne peuvent pas être croisés dans des scénarios différents. Vous ne pouvez pas créer un deuxième scénario de réplication utilisant le répertoire maître et le répertoire racine utilisés pour votre premier scénario.
- Paramètres de haute disponibilité pour un hôte UNIX/Linux :
  - Informations système : les propriétés de contrôleur de domaine d'Active Directory et de MS Cluster ne sont pas prises en charge. Les valeurs sont donc toujours définies sur *Non*. Dans le cas de la propriété du serveur DNS, seul le processus de serveur BIND *named* est vérifié. Si *named* est en cours d'exécution, la propriété de serveur DNS est définie sur *Oui*, autrement, elle est définie sur *Non*.
  - Configuration de réseau : le nom de NetBIOS n'est pas pris en charge.
- Les liens physiques sont désormais pris en charge. Les liens physiques ne peuvent pas être créés entre des systèmes de fichiers différents ou entre des répertoires racines sur le même système de fichiers.
- L'exécution simultanée de plusieurs scénarios à partir de différentes zones non globales sur Solaris n'est pas prise en charge. Cependant, vous pouvez créer plusieurs scénarios à partir de la zone globale Solaris et en gérer tous les scénarios à partir de cette zone.

  Remarque : Assurez-vous que tous les répertoires des zones locales sont accessibles à partir de la zone globale Solaris.

Annexe A : Fichiers installés

Lors de l'installation de CA ARCserve RHA, différents fichiers sont installés pour différents systèmes d'exploitation, tels que décrits dans les sections ci-dessous.

Ce chapitre traite des sujets suivants :

Fichiers installés sous Red Hat Linux Enterprise et Novell SUSE Linux Enterprise

Pour les plates-formes Linux, les fichiers ci-dessous sont installés.

Fichier installé	**Description**
/opt/CA/ARCserveRHA/bin/ws_rep	En mode utilisateur, le moteur CA ARCserve RHA fonctionne comme un démon. Sa principale responsabilité consiste à collaborer avec le module kernel xofs (filtrage du système), pour suivre les modifications du système de fichiers et propager ces modifications en fonction du scénario de réplication.
/opt/CA/ARCserveRHA/kernel/fs/xofs.*	Système de fichiers propriétaire - *xofs*. Implémenté sous la forme d'un module kernel chargeable. L'objectif principal de xofs consiste à suivre les modifications du système de fichiers et à les notifier au moteur. Il est chargé au démarrage du système (via /etc/init.d/CA ARCserve RHA). **Remarque :** *.up* est utilisé pour un monoprocesseur tandis que *.smp* l'est pour un multiprocesseur symétrique.
/etc/init.d/ARCserveRHA	Script de démarrage utilisé pour démarrer et arrêter le moteur.
/etc/pam.d/ws_rep	Requis par CA ARCserve RHA pour authentifier les connexions de gestion de l'interface utilisateur graphique.

/opt/CA/ARCserveRHA/bin/README	Fichier Readme de CA ARCserve RHA
/opt/CA/ARCserveRHA/bin/ws_rep.cfg	Fichier de configuration de CA ARCserve RHA
/opt/CA/ARCserveRHA/bin/uninstall.sh	Script de désinstallation du logiciel.

Fichiers installés sur IBM AIX

Pour les plates-formes AIX, les fichiers ci-dessous sont installés.

Fichier installé	**Description**
/opt/CA/ARCserveRHA/bin/ws_rep	En mode utilisateur, le moteur CA ARCserve RHA fonctionne comme un démon. Sa principale responsabilité consiste à collaborer avec le module kernel xofs (filtrage du système), pour suivre les modifications du système de fichiers et propager ces modifications en fonction du scénario de réplication.
/opt/CA/ARCserveRHA/bin/xofs.ext	Système de fichiers propriétaire - *xofs*. Implémenté sous la forme d'une extension kernel chargeable. L'objectif principal de xofs consiste à suivre les modifications du système de fichiers et à les notifier au moteur. Il est chargé au démarrage du système (via /opt/CA/ARCserveRHA/bin/ARCserveRHA.rc).
/opt/CA/ARCserveRHA/bin/xoctl	Utilitaire auxiliaire (aide de système de fichiers). Précharge xofs lors du démarrage du système.
/opt/CA/ARCserveRHA/bin/xoumount	Utilitaire auxiliaire (*démonte xofs*). Utilitaire analogue à la ligne de commande *umount* standard. **Remarque :** Dans la version actuelle de CA ARCserve RHA, la commande *umount* standard n'est pas prise en charge par xofs.
/opt/CA/ARCserveRHA/bin/ARCserveRHA.rc	Script de démarrage utilisé pour démarrer et arrêter le moteur.
/opt/CA/ARCserveRHA/bin/uninstall.sh	Script de désinstallation du logiciel.

Fichiers installés sur Solaris

Pour les plates-formes Solaris, les fichiers ci-dessous sont installés.

Fichier installé	**Description**
/opt/CA/ARCserveRHA/bin/ws_rep	En mode utilisateur, le moteur CA ARCserve RHA fonctionne comme un démon. Sa principale responsabilité consiste à collaborer avec le module kernel xofs (filtrage du système), pour suivre les modifications du système de fichiers et propager ces modifications en fonction du scénario de réplication.
/usr/kernel/fs/xofs et /usr/kernel/fs/sparcv9/xofs	Système de fichiers propriétaire - *xofs*. Implémenté sous la forme d'un module kernel chargeable. L'objectif principal de xofs consiste à suivre les modifications du système de fichiers et à les notifier au moteur. Chargé à la demande lors du démarrage du scénario de réplication.
/opt/CA/ARCserveRHA/bin/uninstall.sh	Script de désinstallation du logiciel.
/opt/CA/ARCserveRHA/bin/configure.sh (zones)	Permet de configurer ws_rep dans des zones non globales.

Annexe B : Dépannage

Les informations suivantes sont fournies pour vous permettre de dépanner les scénarios CA ARCserve RHA pour UNIX/Linux.

- Cette version de CA ARCserve RHA propose une fonction permettant de décharger xofs automatiquement, même si certains fichiers sont ouverts lors de l'opération d'arrêt du scénario.

Ce chapitre traite des sujets suivants :

Déchargement des pilotes xofs

Si certains répertoires ont été laissés par inadvertance sous contrôle xofs pendant la procédure de désinstallation (par exemple, le scénario s'exécutait et le répertoire était monté par xofs), cette procédure ne peut pas décharger le pilote xofs de votre système.

Dans ce cas, vous pouvez simplement redémarrer l'ordinateur ou décharger le pilote xofs manuellement.

Pour décharger les pilotes xofs

1. Vérifiez s'il y a des points de montage xofs à l'aide de la commande suivante :

   ```
   #cat /etc/xofs_mnttab
   ```

2. Arrêtez tous les processus qui bloquent votre répertoire. Utilisez la commande *fuser* appropriée pour votre plate-forme afin de détecter les processus qui ont des fichiers ouverts dans votre répertoire :

   AIX et Solaris

   ```
   #fuser -c <dir_from_xofs_mnttab>
   ```

   Linux

   ```
   #fuser -u <dir_from_xofs_mnttab>
   ```

3. Utilisez la commande *umount* pour le répertoire détecté à l'étape 1.

   ```
   #umount <rép_listé_par_xofs_mnttab>
   ```

4. Vérifiez qu'aucun processus n'utilise le pilote xofs et déchargez celui-ci manuellement. Suivez les instructions appropriées pour votre plate-forme :

   AIX

   Exécutez la commande suivante en tant qu'utilisateur root afin de vérifier si xofs est chargé dans le noyau :

   ```
   echo lke | kdb| grep xofs
   ```

   Exécutez la commande suivante en tant qu'utilisateur root afin de décharger le pilote xofs :

   ```
   /opt/CA/ARCserveRHA/bin/xoctl u /opt/CA/ARCserveRHA/bin/xofs.ext
   ```

   Solaris

   Exécutez la commande suivante afin de vérifier si le pilote est chargé dans la mémoire :

   ```
   modinfo|grep xofs
   ```

   Exécutez la commande suivante manuellement afin de décharger le pilote xofs :

   ```
   modunload -i <ID xofs>
   ```

   Linux

   Exécutez la commande suivante afin de vérifier que la valeur du compteur de référence du pilote xofs est 0 :

   ```
   /sbin/lsmod|grep xofs
   ```

   Exécutez la commande suivante manuellement afin de décharger le pilote xofs :

   ```
   /sbin/rmmod xofs
   ```

Index